CRYPTANALYSIS ASPECTS IN 3-D WATERMARKING

V. Itier[1,3], *W. Puech*[1], *A. G. Bors*[2]

[1]LIRMM, UMR 5506 CNRS, University of Montpellier 2, MONTPELLIER, FRANCE
[2]Dept. of Computer Science, University of York, YORK YO10 5GH, UK
[3]STRATEGIES S.A, 41-43 rue de Villeneuve, Parc des Affaires SILIC, 94583 RUNGIS FRANCE

ABSTRACT

3-D object security is increasingly brought to the attention of the public by the expansion of new multimedia technologies such as the 3-D printing. In the development of crypto-security systems of 3-D objects, we can identify two major directions represented by the cryptography and digital watermarking. A good security system has to be format compliant, has to preserve the original bit rate and, whenever possible, it should be reversible. Watermarking methodology has the advantage of ensuring that the embedded hidden message can be verified at any processing stage such as the transmission, storage and when visualizing the embedding media. In this paper, we review the previous work in 3-D security and analyze the crypto-security of a 3-D watermarking method which embeds information by mesh surface distortion minimization. Then, we discuss future avenues of research by presenting emerging applications.

Index Terms— 3-D watermarking, 3-D encryption, cryptanalysis, emerging applications.

1. INTRODUCTION

Because of the expansion of new technologies including mobile multimedia and 3-D printing, there is an increasing requirement for developing efficient 3-D security systems. The creators and owners of 3-D data are faced with a rising tide of challenges, including that of losing their copyright rights, during the transmission, visualization, storage, modification, printing or sharing. A large variety of activity sectors are interested in various applications of 3-D object security. For example, artistic creators of 3-D art and designers of 3-D objects using CAD (computer-aided design) extensively used nowadays in virtual reality, computer games and other applications, want to preserve their copyright. In medical imaging, 3-D data could contain confidential patient information which should not be modified or made available to unauthorized parties. Furthermore, the security of 3-D data is important for the sale of 3-D objects, their outsourcing, 3-D visualization, 3-D online video games, video-conference or video protection.

Unlike the security methodology developed for sounds, images or video, the 3-D security is a relatively new field which started in late '90s. 3-D watermarking has to enforce a series of requirements, such as the invisibility of changes produced to the objects, high capacity, robustness to various attacks, including desynchronization for example, and to be crypto-secure as well. When enforcing any of these requirements in a 3-D watermarking method, we limit the effectiveness of all the others. 3-D security methods are very specific, but they have to work under the Kerckhoffs' principle [1]. Kerckhoff's principle assumes that encryption and watermarking systems rely upon algorithms which are known and available to the world at large. The security is ensured by a secret key which remains confidential and to be known only to the sender and the receiver which use it for encrypting, decrypting, embedding or extracting the message. Kalker defines the watermark security as the inability by unauthorized users to have access to the raw watermarked channel in [2]. Cayre *et al.* [3] links the Shannon's definition of security in cryptographic systems to watermarking [4], while Perez-Freire *et al.* discuss various crypto-attack methodologies that can be attempted against watermarked media in general in [5]. Security in the context of spread-spectrum watermarking system is discussed both theoretically and in practical terms in [6]. Security is understood in [6] as the difficulty of estimating secret parameters of the embedding function based on the observation of watermarked data. The embedded watermark is supposed to resist a large variety of possible attacks including noise addition, geometric attacks, cropping, remeshing, simplification and so on. This is a very challenging requirement since the robustness to one attack will usually fail to secure robustness against the others, [7, 8, 9]. Developing 3-D watermarking algorithms, which would maximize watermark invisibility, robustness to attacks, high bit capacity embedding and high security is extremely challenging for all existing methods, because any improvement in coping with one of these requirements tends to decrease the effectiveness of all the others.

In this paper, we provide a study about how to improve the crypto-security of 3-D watermarking methods. We provide the aims of a 3-D security system, the reason why they are designed and what kind of security levels are needed. We explain how visual confidentiality can be achieved by encrypting or by watermarking methodology for authentication and perceptual integrity. We analyse the perceptual impact of

these security methods, as well. In Section 2 we present the objectives of 3-D data security. Section 3 details the crypto-analysis of a 3-D watermarking method which enforces the minimization of the distortion introduced in the object surface from [9]. Section 4 shows some emerging applications of 3-D security. Finally, Section 5 concludes the paper and lists some future challenges.

2. 3-D SECURITY OBJECTIVES

Confidentiality, integrity, availability, authentication and non repudiation are among the major objectives in 3-D security applications. Security methods can be blind, semi-blind, or requiring prior knowledge about the object. Furthermore, the protected object has to be format compliant and it should be easily visualized by using a standard viewer. We consider two kind of methods consisting of crypto-encryption and watermarking:

- Encryption methods transform the original data to a format that is not identifiable.
- Watermarking methods hide data in the object in an invisible way.

The security of these methods depends only of a secret key [1]. Encryption is very useful for visual confidentiality as presented in Section 2.1. Watermarking has to be invisible and to preserve the shape of the mesh and can be embedded in the geometry, in the topology or in both. Section 2.2 describes a general approach to robust watermarking which has to resist against a variety of attacks. Fragile watermarking, which should fade away, when changes are performed to the 3-D object, in order to certify its authenticity, is introduced in Section 2.3. Section 2.4 presents some shape quality evaluation methods, which can be used to account for mesh distortion.

2.1. Visual confidentiality

Visual confidentiality can be achieved by masking 3-D data to produce an unintelligible cryptogram to anyone who does not share the key. Partially masking the data can be useful to allow restricted visualization to non sensitive data. Following decryption, the decoded mesh is no longer protected. Nevertheless, a practical approach which is based on shuffling vertex coordinates, is presented in Fig. 1. This full encryption preserves the bounding box of the object.

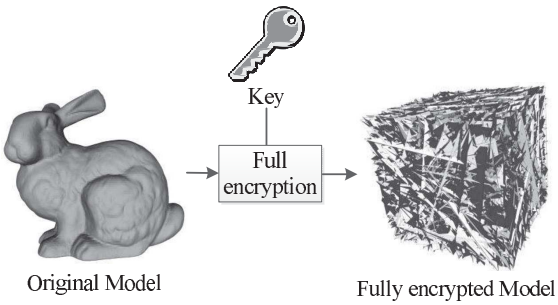

Fig. 1: Classical full encryption scheme.

Selective encryption can be performed by encrypting a part of the mesh or by ciphering the smallest decimals of each vertex, as illustrated Fig. 2. Both methods respect the condition of *format preserving encryption* as explained by Bellare *et al.* [10].

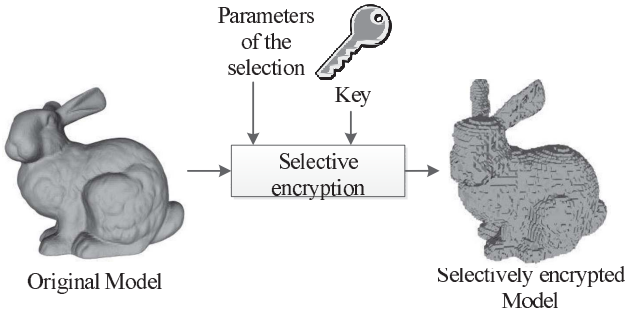

Fig. 2: Classical selective encryption scheme.

It is possible to visualise the results from Fig. 1 and Fig. 2 without knowing the secret key, while the knowledge of the key allows reversibility, leading to the recovery of the original 3-D shape. The encryption of the 3-D object will increase the required rendering time [11]. Selective encryption is sensitive to some attacks such as cropping, remeshing and smoothing attacks.

2.2. Authentication and Copyright

A watermarking scheme can be used to authenticate the 3-D object or to embed a copyright specific signature. In the case of copyright protection, the embedded data would consist of a binary code or a logo, requiring few bits while it can easily identify the owner even if the watermarked object was altered by noise or by some other mesh transformations. For example, robust high capacity watermarking for authentication was proposed by Gao *et al.* [12]. Fig. 3 presents an overview of a classical watermarking method. This figure illustrates the steps for embedding and extracting a logo in order to define the ownership of the object.

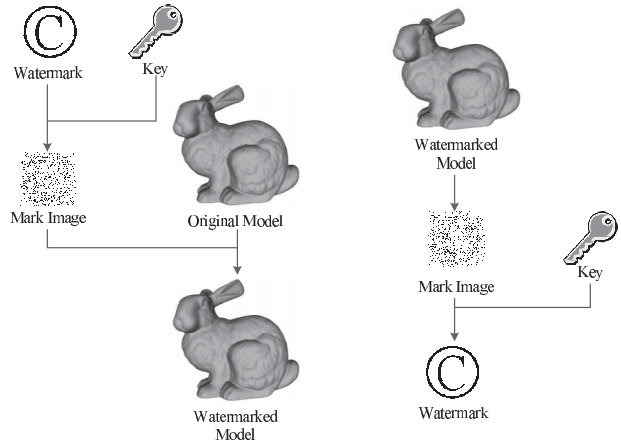

Fig. 3: Classical watermarking scheme.

The protection of copyright ownership has to deal with attackers and the robustness is a very important requirement.

Watermarks should be robust to the following categories of attacks: similarity transformations, signal processing attacks, cropping and connectivity attacks, Wang *et al.* [7]. Assuming a robust watermarking method, this method should be cryp-analysed in order to achieve complete security. Furthermore, for this kind of application, watermarking security could fail against deadlock or collusion attacks.

2.3. Perceptual integrity

Watermarks used for 3-D object authentication are used to ensure the receiver that the integrity of 3-D object has not been altered or changed since its creation. Such watermarks would not require a high capacity embedding and have to be fragile. Moreover, it should be able to locate or to identify the object area which was changed. A challenge to such 3-D watermarks is posed by steganography attack method presented by Bogomjakov *et al.* [13], which reorders the vertices in the mesh file. In many applications, these operations are not considered because they do not affect the mesh. Yeo and Yeung [14] have proposed a method that can deal with vertex reordering. They employ a hash function that calculates two indices for each vertex. They use the position of a vertex and its adjacent vertices to calculate the *location index*. Then, they calculate the *index value* with another hash function based on vertex coordinates. The extraction step can detect modifications by checking differences between the indices. Nevertheless, such authentication methods should have some robustness to the normal manipulation of the 3-D data such as compression.

2.4. Perceptual invisibility and quality metrics

A watermarking method should be invisible and preserve the shape of the mesh. Moreover, the object could have different properties related to its visualization, manipulation, modification. So a good watermarking scheme has to be undetectable and must not affect the user's experience in any way. Various metrics are used for watermarking such that the resulting changes are not visible or they are hidden after embedding. The following metrics have been used for assessing the 3-D shape distortion: the geometric Laplacian (GL) proposed by Karni and Gotsman [15], the signal to noise ratio (SNR), the maximum root mean square error (MRMS) and the Hausdorff distance (HD). MRMS and HD are often computed by using the algorithm Metro proposed in [16] for mesh compression assessment. Peak signal-to-noise ratio (PSNR), between the vertex locations of the stego and original model, was used in [17] for assessing the shape distortions. The Metro measure [16], was used for measuring the 3-D shape similarity for surface simplication algorithms. Bors and Luo proposed a watermarking method based on minimizing a surface distortion function which depended on the sum of distances from the vertices of the watermarked object to the surface of the original object, to the surface of the watermarked object and to the location of the same vertex from the original object in [9]. MOS (mean opinion score) is a measure which assesses 3-D object changes according to the human perception system and was used for the evaluation of other metrics like the mesh structural distortion measure (MSDM2) proposed by Lavoué [18], the Strain Field-based Measure (SF) proposed by Bian *et al.* [19] and the Roughness-based Measures from Corsini *et al.* [20].

3. SECURITY OF 3-D WATERMARKING

The watermark can be seen as a communication channel, which would require an additional layer of security in order to ensure than an unauthorized user would not be able to find the watermark code. Security crypto-attacks against watermarking systems in general can be classified into known message attack (KMA), constant message attack (CMA) and watermarked only attack (WOA) [5, 6]. The KMA assumes that the attacker is able to gather a number of signals watermarked by the same key while assuming known the watermark message for each of them. CMA attack is used when the same watermark code is embedded in different regions of the object [5]. A watermark security approach introduces a series of parameters which would depend on a key, independent on the watermark, known to both the sender and the receiver. Such parameters, depending on secure keys, could correspond to the randomization of the watermarking signal by an additive dithering signal or by controlling the syncronisation of the embedded bits. The limitations of the independent component analysis (ICA) and principal component analysis (PCA) algorithms in breaking the security of the spread spectrum watermarking algorithms was shown in [6]. The effective key length was studied by Furon and Bas in [21] for distortion compensated dither modulation quantized index modulation (QIM) watermarking schemes, where the dither vector plays the role of the secret key. This scheme was shown not to be secure in the context of KMA attacks.

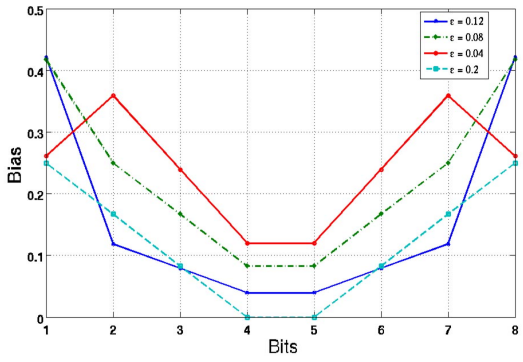

Fig. 4: Error in the estimation of the means for each bin, corresponding to the attempts by a crypto-attacker to find a watermark message. The embedded message is made up of 8 alternating bits of 1 and 0, considering $\varepsilon = 0.15$.

In the following we analyze a security method depending on a single security parameter controlling the syncronisation of the embedded bits as in [9], considering the the Kerckhoffs's principle [1] assumptions. In this method, the vertex norm $\rho_j = \|\mathbf{v}_j - \mathbf{o}\|$, corresponding to the Euclidean distance for a given vertex of location $\mathbf{v}_j$ to the center of the

object, is considered as a statistical variable, representing the signal support for the watermark. The distances to the object's center are ranked and a certain percentage ε of vertices with extreme norms are removed from further calculation. The remaining vertices, corresponding to distances from the center of the object of $\rho_j \in [\rho_{min}, \rho_{max}]$, are split into M bins, each of width $\rho_b = (1-2\varepsilon)(\rho_{max} - \rho_{min})/M$ being associated with a bit which is then statistically embedded, [9]. A crypto-attacker, even knowing the 3-D watermarking method, would need to guess the value of ε, within a certain quantization error, by using exhaustive search. Let us assume in the following that the expectations of the mean for a bin of vertex norms is uniform and consequently $E[\hat{\mu}] = \frac{1}{2}$. Following watermark embedding, the statistical distributions are changed and we consider $E[\hat{\mu}] = \frac{3}{4}$ for embedding a 1 and $E[\hat{\mu}] = \frac{1}{4}$ for a 0. In Fig. 4 we evaluate the error in the estimation of the means for the vertices from the bins, corresponding to each embedded bit, as it is estimated by a crypto-attacker attempting to find the watermark code, when using $M = 8$ alternating bits of 0 and 1 and where the secure key was $\varepsilon = 0.15$. We consider that the attacker tries various values such as $\varepsilon \in \{0.04, 0.08, 0.12, 0.2\}$. A resulting error of $1/4$ or larger, corresponds to a uniform distribution or to a bit flip, due to the overlapping between regions of vertices with norm statistics characteristics for bits of 0 with those for bits of 1. This would result into wrongly estimated bits by the crypto-security attacker. It can be observed from Fig. 4, that due to the symmetry of the trimming, the middle bits are among the most likely to be identified during a crypto-attack. The number of trials, that are required for a crypto-attack on the watermarked object to succeed, depends on how well the attacker can guess the location of half-bins and on the number of embedded bits M and corresponds to $2\varepsilon(\rho_{max} - \rho_{min}))/\rho_b = 2\varepsilon M/(1-2\varepsilon)$. The security of this 3-D watermarking method can be increased by introducing additional key-generated parameters such as for example for controling the localization of the reference **o** and by introducing assymetric trimming of the extremes.

4. OTHER EMERGING APPLICATIONS

In this section we discuss some emerging applications for 3-D data security, including the security of video games, confidentiality of medical patient data, the commercial trading of 3-D objects as well as the protection of the creativity of graphical artists work. Trick *et al.* [22] have proposed a blind and robust algorithm for 3-D video games. Their watermark method is based on modifying the distribution of vertex norms on a coarse version of the mesh model. The vertices are clustered in bins which are protected by using a secret key used for initializing a specific bin mapping. In the context of medical imaging, one could use a 3-D security system for checking data integrity or confidentiality. For example, Jacinto *et al.* [23] have proposed a tool for the 3-D visualization and the interactive selection of medical images using a web interface. The system can reconstruct the segmented anatomical structures for 3-D visualization and manipulation. The resulting mesh could be further encrypted to maintain confidentiality while being stored. Video conferencing is becoming an increasingly used tool. The current trend is to develop video conferencing systems which provide avatars for speakers as the method presented by Eisert and Girod [24], thus allowing multiple channels for transmitting the information while addressing large audiences. The representation of such avatars would require appropriate protective tools in order to ensure their authenticity as well as the confidentiality in protecting the images of people.

Another important emerging application is that of protecting the patent of designs of CAD objects or that of the artwork created by graphical artists in the age of mobile media devices and of 3-D printing. Artists of 3-D graphics do not want to have any sort of changes performed to their works-of-art. While the assumed tolerance can be used to limit the level of distortion following the embedding of specific codes, a better solution is represented by embedding reversible watermarks as for example proposed by Wu and Dugelay [25]. Symmetrical embeddings which produce changes that can be used to cancel each other, represent a solution in this case. Nevertheless, reversible watermarking is more exposed to crypto-security threats and would provide a lower bit capacity and less robustness. 3-D objects are increasingly offered for sale on virtual markets. Computer game and virtual reality companies, as well as other interested parties which do not have the time or the expertise to develop 3-D models themselves, are increasingly the customers for such markets dominated by outsourcing trends. Such markets are not regulated at the moment and 3-D models may be resold by the new owners without the consent of their producer. For example this problem can be addressed by embedding several secure levels of changes into the 3-D object.

5. CONCLUSION

In this paper we provide a short overview of the trends in 3-D object security. After introducing 3-D data cryptography and 3-D watermarking we analyze their requirements and properties, and we discuss various challenges to these methodologies. We provide a short presentation of various quality metrics used for the analysis of 3-D shape changes and their perception by the human visual system. The cryptanalysis of a recently proposed 3-D watermarking system is then analyzed by assuming the Kerckhoffs's principle, according to which the algorithm is entirely known. In this study we assess how random parameters, defined by specific keys, can be used to secure the watermark code. We also discussed various metrics for assessing the surface distortion of 3-D objects. 3-D data security has a wide implication in many areas including those addressing the confidentiality of medical data, virtual reality applications and games, teleconferencing avatars, the protection of CAD objects as well as those produced by the graphical artists in the context of expanding 3-D printing and of mobile multimedia applications.

6. REFERENCES

[1] A. Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires*, vol. IX, pp. 5–38, Jan. 1883.

[2] T. Kalker, "Considerations on watermarking security," in *IEEE Workshop on Multimedia Signal Processing*, 2001, pp. 201–206.

[3] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: theory and practice," *IEEE Transactions on Signal Processing,*, vol. 53, no. 10, pp. 3976–3987, 2005.

[4] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal, Vol 28, pp. 656715*, 1949.

[5] L. Perez-Freire, F. Perez-Gonzalez, T. Furon, and P. Comesana, "Security of lattice-based data hiding against the known message attack," *IEEE Trans. on Information Forensics and Security*, vol. 1, no. 1, pp. 421–439, 2006.

[6] L. Perez-Freire and F. Perez-Gonzalez, "Spread spectrum watermark security," *IEEE Trans. on Information Forensics and Security*, vol. 4, no. 1, pp. 2–24, 2009.

[7] K. Wang, G. Lavoué, F. Denis, and A. Baskurt, "A comprehensive survey on three-dimensional mesh watermarking," *IEEE Transactions on Multimedia*, vol. 10, no. 8, pp. 1513–1527, December 2008.

[8] P. R. Alface and B. Mack, "From 3d mesh data hiding to 3d shape blind and robust watermarking: A survey," in *Transactions on Data Hiding and Multimedia Security II*, ser. LNCS, Y. Q. Shi, Ed., 2007, vol. 4499, pp. 91–115.

[9] A. G. Bors and M. Luo, "Optimized 3D watermarking for minimal surface distortion," *IEEE Trans on Image Processing*, vol. 22, no. 5, pp. 1822–1835, 2013.

[10] M. Bellare, T. Ristenpart, P. Rogaway, and T. Stegers, "Format-preserving encryption." in *Selected Areas in Cryptography*, ser. LNCS, vol. 5867, 2009, pp. 295–312.

[11] M. Eluard, Y. Maetz, and G. Doerr, "Geometry-preserving encryption for 3D meshes," in *Proc. of the IEEE Int. Conference on Image Processing*, 2014.

[12] X. Gao, C. Zhang, Y. Huang, and Z. Deng, "A robust high-capacity affine-transformation-invariant scheme for watermarking 3d geometric models," *ACM Transaction on Multimedia Computing, Communications and Applications*, vol. 8, no. 2S, pp. 34:1–34:21, 2012.

[13] A. Bogomjakov, C. Gotsman, and M. Isenburg, "Distortion-free steganography for polygonal meshes," in *Computer Graphics Forum*, vol. 27, no. 2, 2008, pp. 637–642.

[14] B.-L. Yeo and M. Yeung, "Watermarking 3D objects for verification," *IEEE Computer Graphics and Applications*, vol. 19, no. 1, pp. 36–45, 1999.

[15] Z. Karni and C. Gotsman, "Spectral compression of mesh geometry," in *Proc. of the 27th Annual Conference on Computer Graphics and Interactive Techniques*, ser. SIGGRAPH, 2000, pp. 279–286.

[16] P. Cignoni, C. Rocchini, and R. Scopigno, "Metro: Measuring error on simplified surfaces," Tech. Rep., 1996.

[17] M.-W. Chao, C.-H. Lin, C.-W. Yu, and T.-Y. Lee, "A high capacity 3D steganography algorithm," *IEEE Transactions on Visualization and Computer Graphics*, vol. 15, no. 2, pp. 274–284, 2009.

[18] G. Lavoué, "A multiscale metric for 3D mesh visual quality assessment," *Computer Graphics Forum*, vol. 30, no. 5, pp. 1427–1437, 2011.

[19] Z. Bian, S.-M. Hu, and R. Martin, "Evaluation for small visual difference between conforming meshes on strain field," *Journal of Computer Science and Technology*, vol. 24, no. 1, pp. 65–75, 2009.

[20] M. Corsini, E. Gelasca, T. Ebrahimi, and M. Barni, "Watermarked 3-D mesh quality assessment," *IEEE Transactions on Multimedia*, vol. 9, no. 2, pp. 247–256, 2007.

[21] T. Furon and P. Bas, "A new measure of watermarking security applied on qim," in *Proc. of Information Hiding, LNCS vol. 7692*, 2013, pp. 207–223.

[22] D. Trick, W. Berchtold, M. Schäfer, and M. Steinebach, "3D watermarking in the context of video games," in *IEEE Workshop on Multimedia Signal Processing*, 2013, pp. 418–423.

[23] H. Jacinto, R. Kéchichian, M. Desvignes, R. Prost, and S. Valette, "A web interface for 3D visualization and interactive segmentation of medical images," in *Proc. of the Int. Conf. on 3D Web Technology*, 2012, pp. 51–58.

[24] P. Eisert and B. Girod, "Analyzing facial expressions for virtual conferencing," *IEEE Computer Graphics and Applications*, pp. 70–78, 1998.

[25] H.-T. Wu and J.-L. Dugelay, "Reversible watermarking of 3D mesh models by prediction-error expansion," in *IEEE Workshop on Multimedia Signal Processing*, 2008, pp. 797–802.